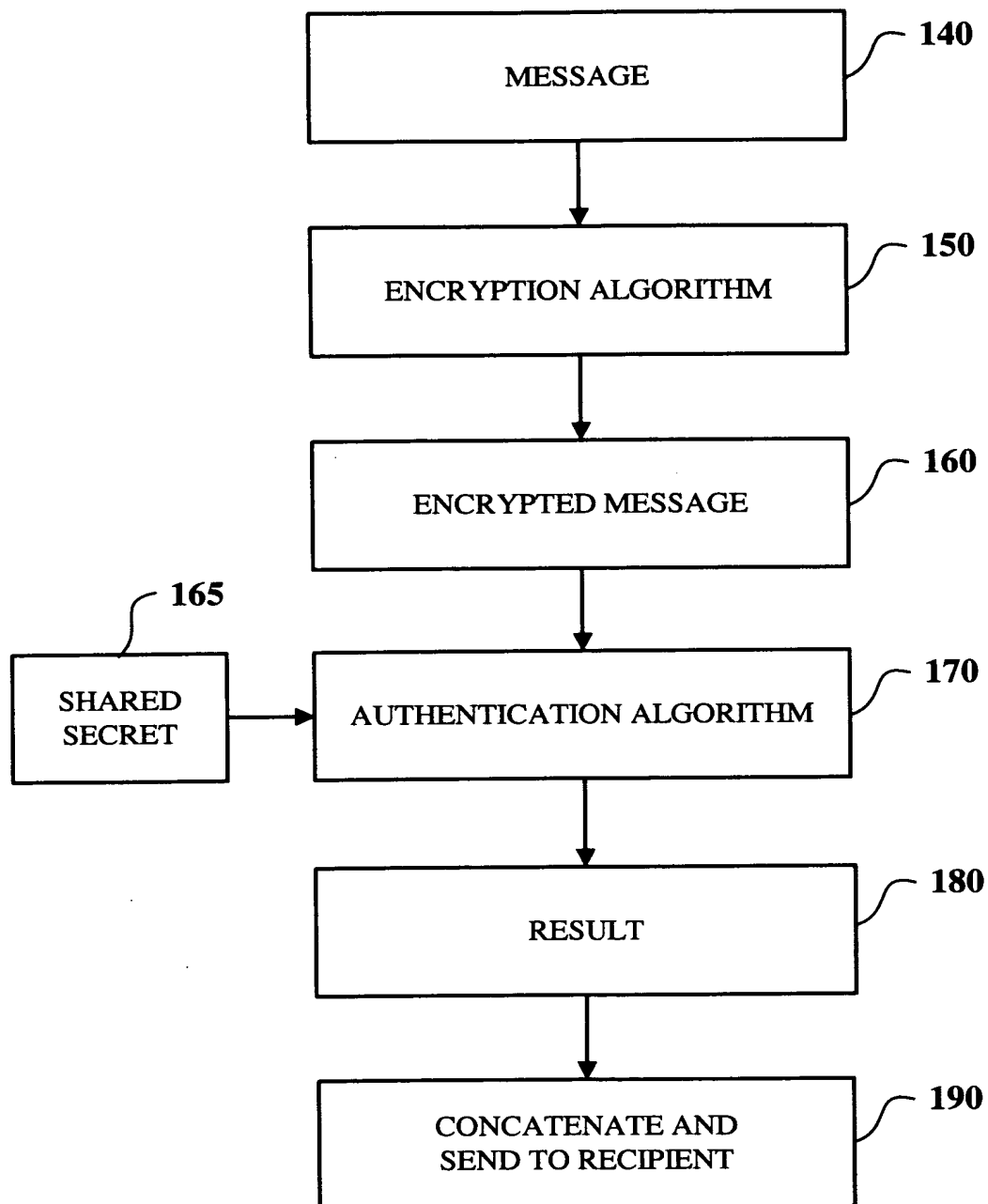
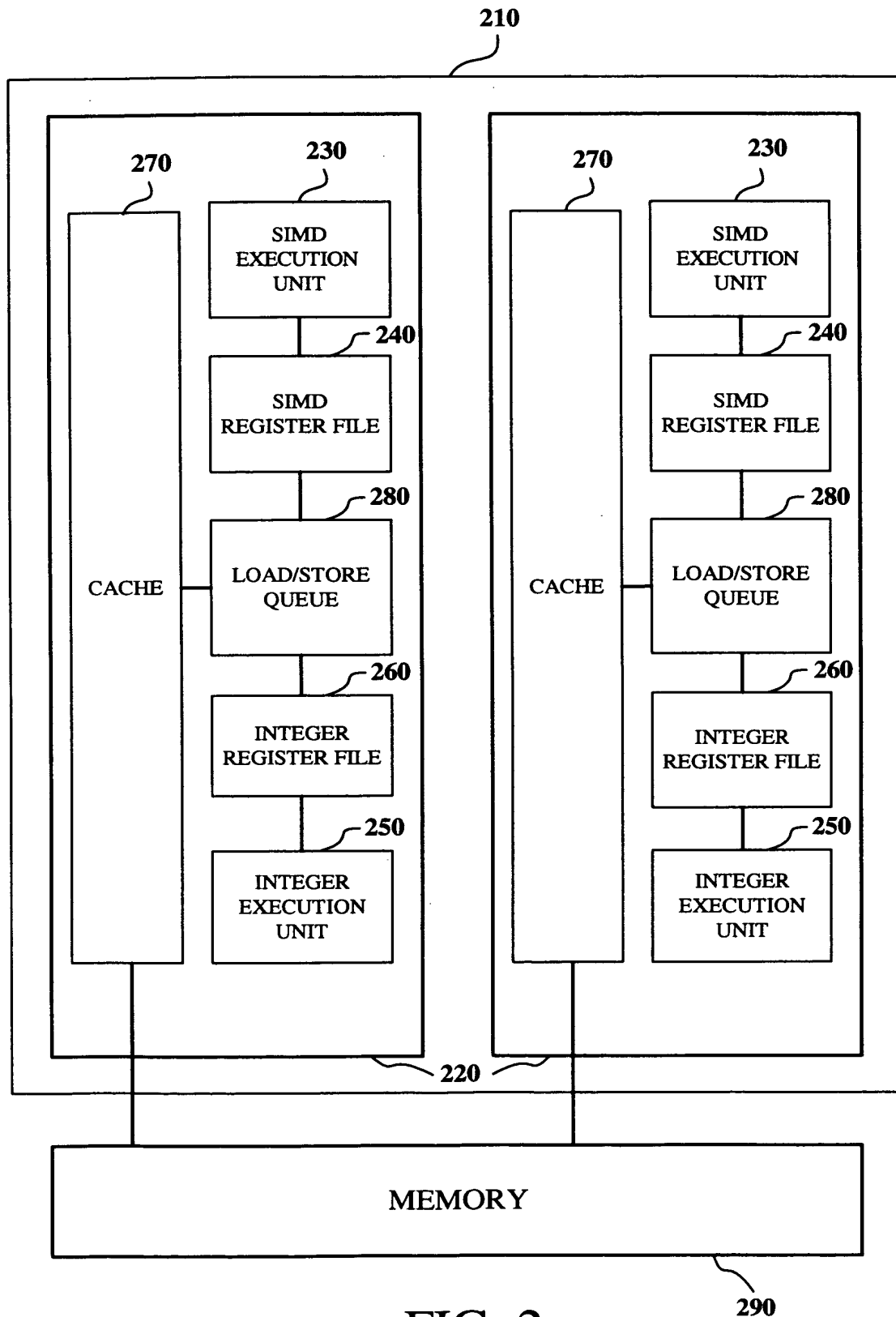


**FIG. 1A**  
(PRIOR ART)



**FIG. 1B**



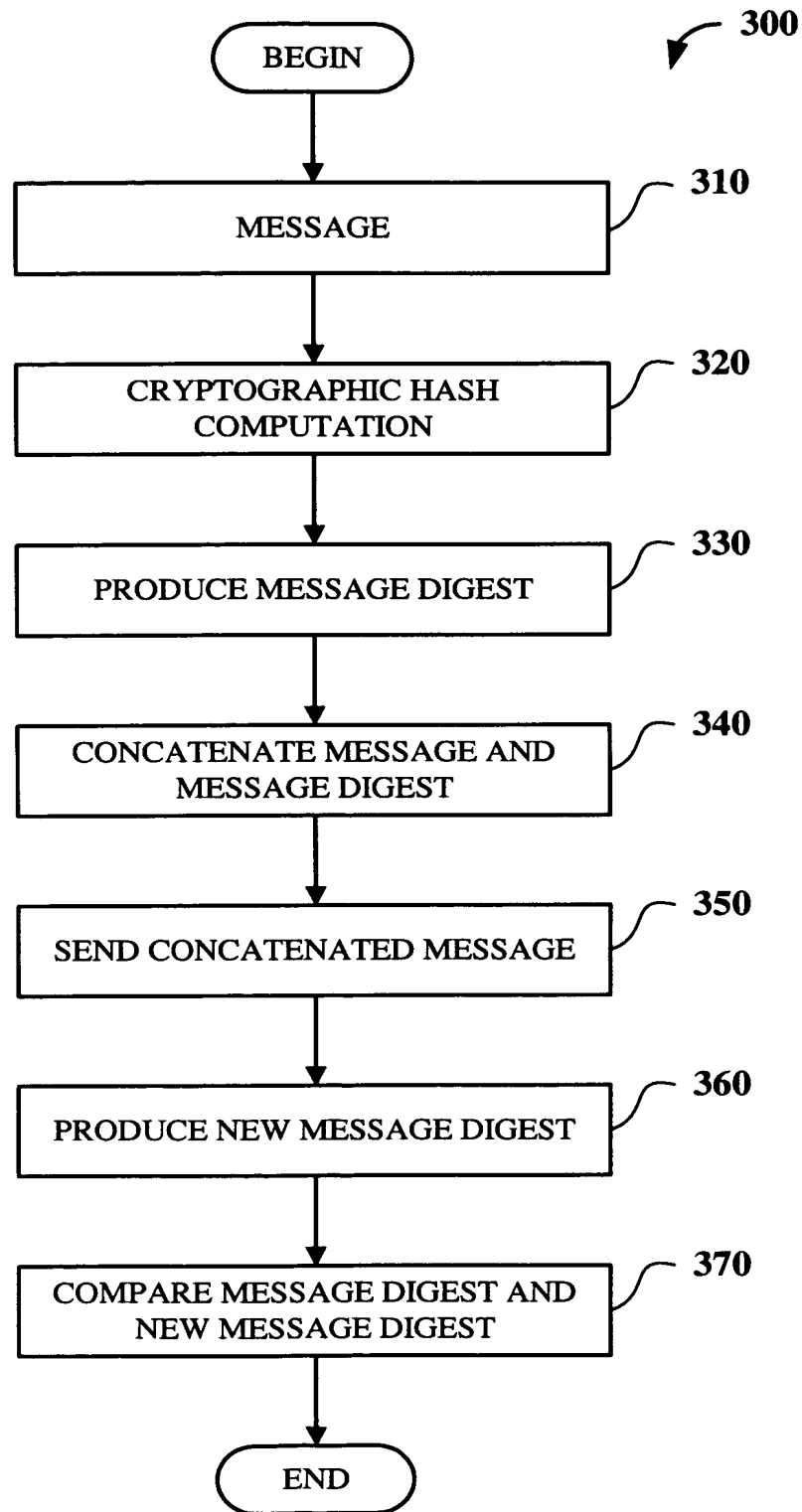
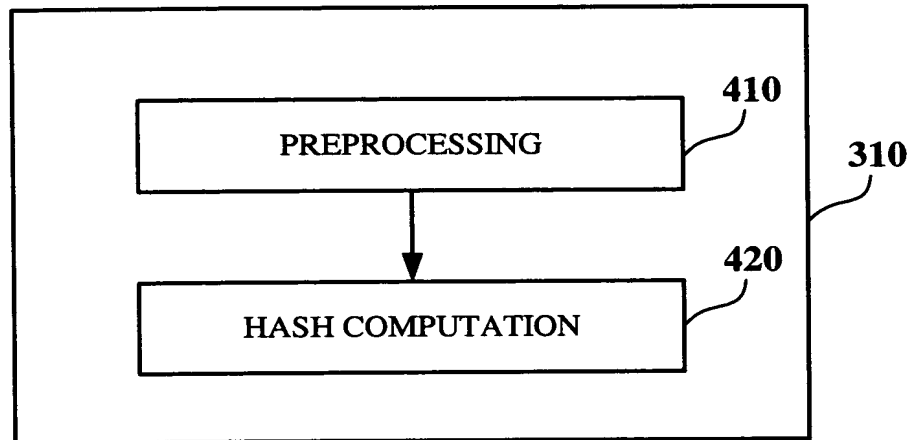
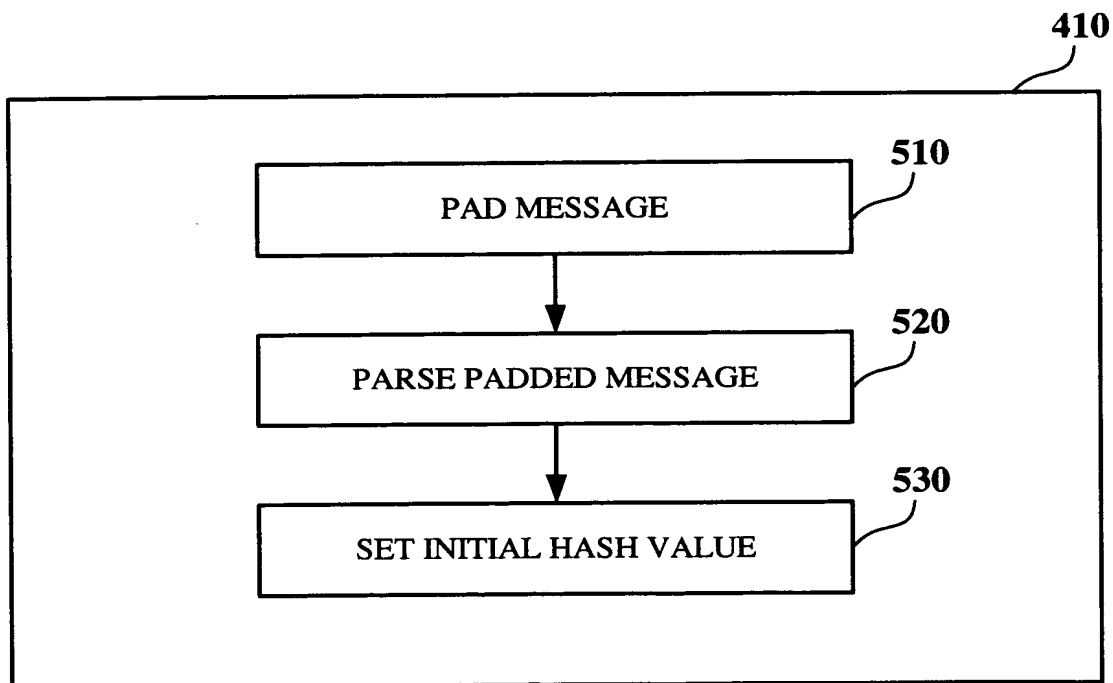


FIG. 3



**FIG. 4**



**FIG. 5**

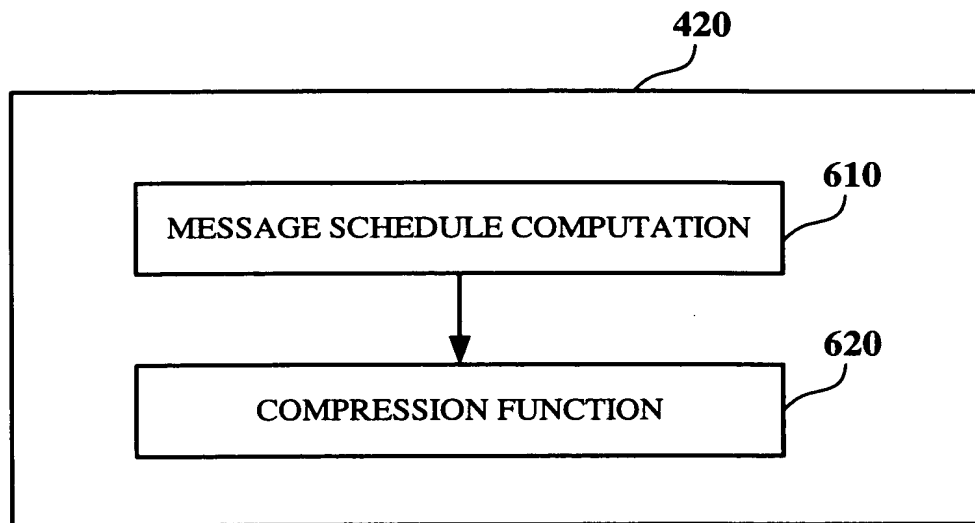


FIG. 6

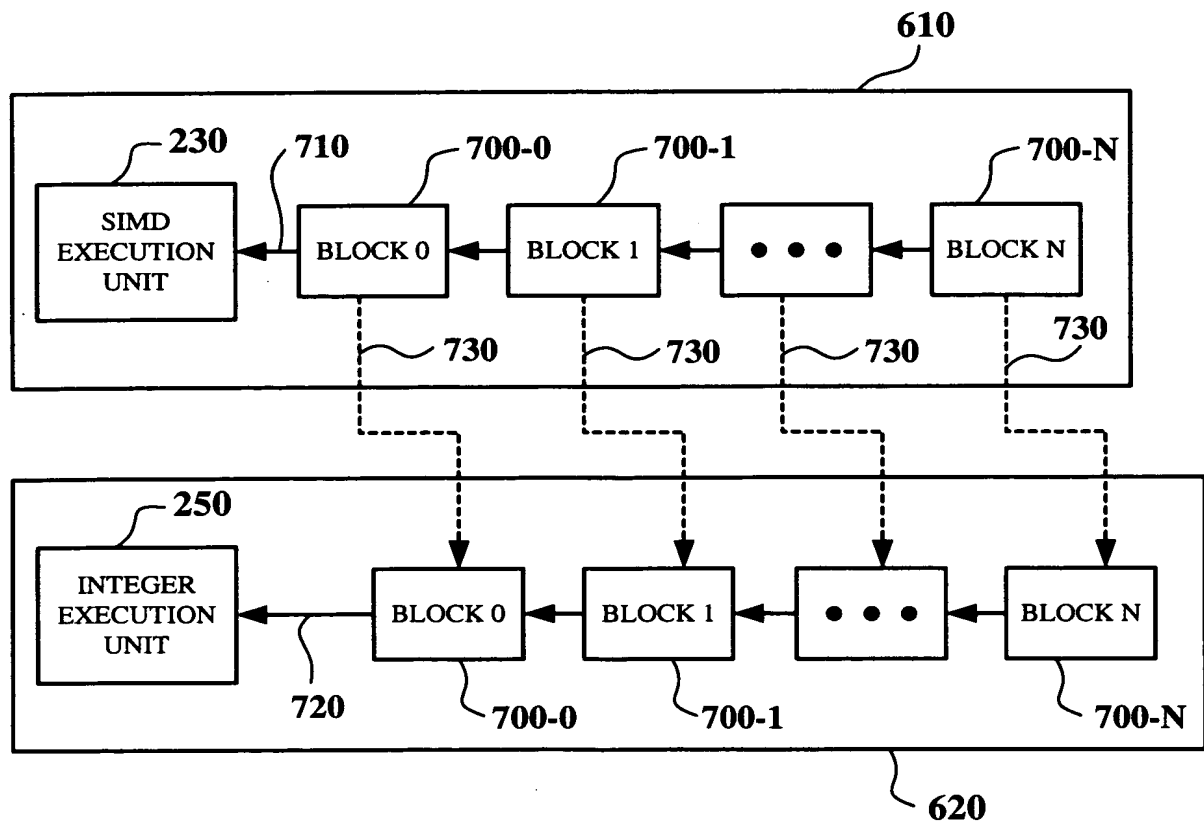


FIG. 7

800

```

Wj = Mj for j = 0 to 15
for j = 16 to 79
{
    Wj = Rot11 (Wj-3 ⊕ Wj-8 ⊕ Wj-14 ⊕ Wj-16)
}

```

FIG. 8A

850

```

for j = 0 to 79
{
    T = rot15(a) + fj (b,c,d) + e + kj + wj
    e = d
    d = c
    c = rot130(b)
    b = a
    a = T
}
where:
    fj (x,y,z)    = (x&y) ⊕ (~x&z)
                  = x ⊕ y ⊕ z
                  = (x&y) ⊕ (x&z) ⊕ (y&z)
                  = x ⊕ y ⊕ z
    for j = 0 to 19
    for j = 20 to 39
    for j = 40 to 59
    for j = 60 to 79

kj = 0x5a827999
   = 0x6ed9ebal
   = 0x8f1bbcdc
   = 0xca62c1d6
    for j = 0 to 19
    for j = 19 to 39
    for j = 40 to 59
    for j = 60 to 79

```

FIG. 8B

900

```

Wj = Mj for j = 0 to 15
for j = 16 to 63
{
    Wj = S1 (Wj-2) + Wj-7 + S0 (Wj-15) + Wj-16
}

```

where:

$S0(x) = \text{Rotr}7(x) \wedge \text{Rotr}18(x) \wedge \text{Shr}3(x)$   
 $S1(x) = \text{Rotr}17(x) \wedge \text{Rotr}19(x) \wedge \text{Shr}10(x)$

FIG. 9A

950

```

for j = 0 to 63
{
    T1 = h + sig1(e) + ch(e,f,g) + kj + Wj
    T2 = sig0(a) + maj(a,b,c)
    h = g
    g = f
    f = e
    e = d + T1
    d = c
    c = b
    b = a
    a = T1 + T2
}

```

where:

$\text{sig}0(e) = \text{rotr}2(e) \oplus \text{rotr}13(e) \oplus \text{rotr}22(e)$   
 $\text{sig}1(a) = \text{rotr}6(a) \oplus \text{rotr}11(a) \oplus \text{rotr}25(a)$   
 $\text{ch}(e,f,g) = (e \& f) \oplus (\sim e \& g)$   
 $\text{maj}(a,b,c) = (a \& b) \oplus (a \& c) \oplus (b \& c)$

FIG. 9B



1000

```
Wj = mj for j = 0 to 15
for j = 16 to 79
{
  Wj = gamma1(Wj-2) + Wj-7 + gamma0(tj-15) + Wj-16
}
```

where:

```
gamma0(x) = rotr1(x) ⊕ rotr8(x) ⊕ shr7(x)
gamma1(x) = rotr19(x) ⊕ rotr61(x) ⊕ shr6(x)
```

FIG. 10A

1050

```
for j = 0 to 79
{
  T1 = h + sig1(e) + ch(e,f,g) + kj + wj
  T2 = sig0(a) + maj(a,b,c)
  h = g
  g = f
  f = e
  e = d + T1
  d = c
  c = b
  b = a
  a = T1 + T2
}
```

where:

```
sig0(e) = rotr28(e) ⊕ rotr34(e) ⊕ rotr39(e)
sig1(a) = rotr14(a) ⊕ rotr18(a) ⊕ rotr41(a)
ch(e,f,g) = (e&f) ⊕ (~e&g)
maj(a,b,c) = (a&b) ⊕ (a&c) ⊕ (b&c)
```

FIG. 10B